

Analytic difference rings

Thomas Scanlon*

Abstract. Generalizing and synthesizing earlier work on the model theory of valued difference fields and on the model theory of valued fields with analytic structure, we prove Ax–Kochen–Eršov style relative completeness and relative quantifier elimination theorems for a theory of valuation rings with analytic and difference structure. Specializing our results to the case of $W[\mathbb{F}_p^{\text{alg}}]$, the ring of Witt vectors of the algebraic closure of the field with p elements, given together with the relative Frobenius and the Tate algebras as analytic structure, we develop a model theoretic account of Buium’s p -differential functions. In so doing, we derive a uniform p -adic version of the Manin–Mumford conjecture.

Mathematics Subject Classification (2000). Primary 03C10, 03C60, 12J10; Secondary 11D45, 11G10, 12H10, 13K05.

Keywords. Ax–Kochen–Eršov principle, difference ring, p -differential function, Witt vectors, abelian varieties, Manin–Mumford conjecture.

1. Introduction

If (K, v) is a complete valued field and $f(x_1, \dots, x_n) = \sum a_\alpha x^\alpha \in K[[x_1, \dots, x_n]]$ is a formal power series over K for which $v(a_\alpha) \rightarrow \infty$ as $|\alpha| \rightarrow \infty$, then f defines a function $\mathcal{O}_K^n \rightarrow K$. Considering a formal first-order language rich enough to express the field structure, the binary relation $v(x) \leq v(y)$ and the functions coming from such convergent power series, one has a natural logical setting for studying nonarchimedean analysis. If one includes in addition a unary function symbol σ to denote a field automorphism which respects the valuation in the sense that $v(x) = v(\sigma(x))$ universally and respects the analytic structure in the sense that $\sigma(f(x)) = f^\sigma(\sigma(x))$ where f^σ denotes the effect of applying σ to the coefficients of f , then one has a strong enough language to study analytic difference rings, the central object of consideration in this paper.

While we have several motivations to study these structures, two stand out most prominently. First, following the seminal work of Ax and Kochen [1], [2], [3] and Eršov on the model theory of valued fields, a great many results showing that valued fields considered in ever more complicated languages have very elegant theories have been proven. With this work we amalgamate two different strands of the model theory of enriched valued fields. Namely, we show that the theories of valued fields with analytic structure and of valued difference fields may be unified. Further unification is

*Partially supported by an NSF CAREER award.

certainly possible. Routine modifications of the proofs presented here should suffice to combine analytic and differential structure, or more generally D -structure, while other extensions will require the development of genuinely new methods. Secondly, we wish to give a model theoretic account of Buium's theory of p -differential geometry and thereby deduce uniformities in Diophantine geometry through applications of the compactness theorem and appropriate quantifier elimination theorems.

Let us recall a little of the theory of p -differential operators. For p a prime number a p -derivation δ on a commutative ring R is a function $\delta: R \rightarrow R$ satisfying

- $\delta(1) = 0$,
- the functional equation $\delta(x + y) = \delta(x) + \delta(y) + \Phi_p(x, y)$ where $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$ is the integral polynomial $\frac{1}{p}(X^p + Y^p - (X + Y)^p)$, and
- the functional equation $\delta(xy) = y^p\delta(x) + x^p\delta(y) + p\delta(x)\delta(y)$.

Given a p -derivation $\delta: R \rightarrow R$ one can define a ring endomorphism $\sigma: R \rightarrow R$ by the equation $\sigma(x) := x^p + p\delta(x)$. Conversely, if p is not a zero divisor in R and $\tau: R \rightarrow R$ is an endomorphism lifting the Frobenius in the sense that $\tau(x) \equiv x^p \pmod{p}$ for all $x \in R$, then $\tilde{\delta}: R \rightarrow R$ defined by $\tau(x) = x^p + p\tilde{\delta}(x)$ is a p -derivation.

As with differential algebra, there is a p -differential geometry associated to the category of rings with p -derivations. At the naïve level, one can consider sets defined by the vanishing of p -differential polynomials, expressions of the form $P(\mathbf{x}, \dots, \delta^n(\mathbf{x}))$ where P is a polynomial, as the basic affine sets. In the case that the underlying rings are domains, this p -differential geometry is essentially the same as the corresponding difference algebraic geometry coming from difference equations involving σ and there is already a well developed model theoretic approach to this subject [7], [8]. However, a richer geometry more in line with that of Kolchin's differential algebraic geometry may be obtained by p -adically completing the rings of p -differential polynomials. Indeed, Buium notes that to globalize p -differential geometry one must consider these p -adically complete rings of operators. The fundamental functions in this theory, the p -differential functions, locally have the form $F(\mathbf{x}, \dots, \delta^n \mathbf{x})$ where $\mathbf{x} = (x_1, \dots, x_m)$ and F is given by p -adically convergent power series in $(n + 1)m$ variables. Buium shows that many arithmetically interesting functions on the $R := W[\mathbb{F}_p^{\text{alg}}]$ -rational points of schemes over R may be expressed locally as p -differential functions where one takes $\delta := \frac{1}{p}(x^p - \sigma(x))$ with $\sigma: R \rightarrow R$ the Witt–Frobenius, the unique lifting of the Frobenius automorphism to an automorphism of the Witt vectors.

One sees from the above local description of p -differential functions, that every p -differential function over R may be expressed as a term in the language with function symbols for p -adically convergent power series over R , the Witt–Frobenius, and the restricted division function $D_p: R \rightarrow R$ defined by $D_p(x) := \frac{x}{p}$ if $x \in pR$ and $D_p(x) := 0$ otherwise. Conversely, if one were to regard all p -differential functions as definable, then all of the above basic functions would be definable as

well. Consequently, the logic of Buium's p -differential functions is that of the first-order structure of the Witt vectors of the algebraic closure of the field of p elements with a function symbol for the Witt–Frobenius and for all p -adic analytic functions.

Even though the goal of understanding p -differential functions guides our work, we must consider structures of a more abstract nature in order to prove our results sufficiently uniformly in order to derive any useful information about p -differential geometry. We achieve these results by axiomatizing the notion of an analytic difference structure on a valued field and then proving relative completeness and relative quantifier elimination theorems for analytic difference rings in the style of the Ax–Kochen–Eršov theorems for pure valued fields.

The essential tool in our analysis is a uniform version of the Weierstraß division theorem. Fortunately for us, this theorem is already known in the case of most interest to us [20]. Using the uniform Weierstraß division theorem we are able to assign an order-degree to an analytic difference equation with respect to which we may carry out inductive proofs.

The present author previously considered the ring $W[\mathbb{F}_p^{\text{alg}}]$ simply as a difference ring in [17], [5] where a simple axiomatization was presented and a quantifier simplification theorem was proven. However, since difference polynomials are intrinsically finitistic objects, we were able to consider more complicated degree relations and worked with a version of Hensel's lemma unavailable in the analytic difference context. The restrictions imposed by considering simultaneously analytic and difference structure have forced us to employ an ostensibly weaker form of Hensel's lemma which miraculously suffices.

This paper is organized as follows. In Section 2 we introduce our basic axioms for analytic difference rings and establish some of the fundamental results about these structures. In Section 3 we state and prove our Ax–Kochen–Eršov theorems for analytically difference henselian rings. In Section 4 we recall the theory of p -differential functions in detail and apply our results of Section 3 to prove a uniform version of the Manin–Mumford conjecture.

2. Foundations of analytic and difference structure

We begin this section by recalling that a *difference ring* (R, σ) is a commutative (unital) ring R given together with a distinguished ring endomorphism $\sigma : R \rightarrow R$. While we shall usually consider rings for which σ is an automorphism, we do not insist upon this condition in our definition of the term difference ring. The model theory of difference fields, namely fields given together with a distinguished endomorphism, and, hence, also of difference domains, has been described by Chatzidakis and Hrushovski [7] and in all characteristics by Chatzidakis, Hrushovski, and Peterzil [8].

For us, a valued difference field is a valued field (K, v) given together with a distinguished automorphism $\sigma : K \rightarrow K$ which respects the valuation in the sense

that the equality $v(\sigma(x)) = v(x)$ holds universally. The model theory of valued difference fields has been developed by Bélair, Macintyre and Scanlon [17], [5].

As mentioned in the introduction, an analytic difference ring is simply the ring of integers of a valued difference field given together with analytic functions for which the distinguished automorphism respects the analytic structure. For a *fixed* complete valuation ring it is easy enough to say what one means by analytic structure. However, if one wishes to express the axioms for the theory of such a ring in a first-order language, it is necessary to formulate “analytic structure” more abstractly. Moreover, even if one is only interested in complete rings, to compare the theories of these rings as analytic structures one requires a uniform language.

We adapt van den Dries’ treatment of analytic Ax–Kochen–Eršov theorems [19] and its refinements by van den Dries, Haskell, Macpherson, Lipshitz and Robinson [20], [15] to the valued difference field setting. While we could restrict our attention to such rings of analytic functions as $\mathbb{Z}[[t]]\langle X_1, \dots, X_n \rangle$ or $W[\mathbb{F}_p^{\text{alg}}]\langle X_1, \dots, X_n \rangle$ without sacrificing the examples of greatest interest, we work with potentially more general rings in order to separate the work on the model theory of analytic functions from difference algebra.

Definition 2.1. A *pre-notion of analyticity*, \mathcal{A} , is given by the data of a commutative ring R and a doubly-indexed sequence of subrings $\mathcal{A}_{m,n} \subseteq R[X][[Y]]$ of the ring of formal power series in the n variables $Y = (Y_1, \dots, Y_n)$ over the polynomial ring in the m variables $X = (X_1, \dots, X_m)$ over R for which

1. $\mathcal{A}_{0,0} = R$,
2. if $m \leq m'$ and $n \leq n'$, then $\mathcal{A}_{m,n}$ is a subring of $\mathcal{A}_{m',n'}$ via the natural inclusion, and
3. \mathcal{A} is closed under compositions as far as this makes sense.

Definition 2.2. Given a pre-notion of analyticity \mathcal{A} , an \mathcal{A} -analytic structure on a valuation ring \mathcal{O} with maximal ideal \mathfrak{m} is given by a sequence of homomorphisms $I_{m,n}: \mathcal{A}_{m,n} \rightarrow \text{Functions}(\mathcal{O}^m \times \mathfrak{m}^n, \mathcal{O})$ which respect the compositional identities in \mathcal{A} , the identities coming from the inclusions $\mathcal{A}_{m,n} \hookrightarrow \mathcal{A}_{m',n'}$, and send the variables X_i and Y_i to the obvious projection maps.

Remark 2.3. If R itself is a complete valuation ring and $\mathcal{A}_{m,n} = R[X][[Y]]$, then the usual interpretation of the elements of $\mathcal{A}_{m,n}$ gives R an \mathcal{A} -analytic structure.

Remark 2.4. In the definition of \mathcal{A} -analytic structure, it is not really necessary that \mathcal{O} be a valuation ring and \mathfrak{m} its maximal ideal. However, this is the only case we consider in our applications.

Remark 2.5. Given a pre-notion of analyticity \mathcal{A} and \mathcal{L} a first-order language for valued fields containing (at least) a sort symbol \mathcal{O} for the valuation ring and a sort symbol \mathfrak{m} for the maximal ideal of the valuation ring we may naturally expand \mathcal{L} to $\mathcal{L}(\mathcal{A})$ by new function symbols where for each $f \in \mathcal{A}_{m,n}$ we have a function

symbol, also denoted f , of domain sort $\mathcal{O}^m \times \mathfrak{m}^n$ and range sort \mathcal{O} . The condition that a particular interpretation of \mathcal{A} on a valuation ring defines an \mathcal{A} -analytic structure may be expressed as a first-order theory in $\mathcal{L}(\mathcal{A})$.

Before we can give our conditions on when a pre-notion of analyticity is actually a notion of analyticity, we must recall some of the basic formalism of quotient operators on valuation rings and leading term structures. In what follows, we use the symbol \mathcal{Q} for our quotient operators even though “ D ” is more common in the literature.

Definition 2.6. Let (K, v) be a valued field with valuation ring $\mathcal{O} := \mathcal{O}_{K,v}$ having the maximal ideal $\mathfrak{m} := \mathfrak{m}_{K,v}$. We define two operators \mathcal{Q}_0 and \mathcal{Q}_1 on \mathcal{O}^2 by $\mathcal{Q}_0(x, y) := \frac{x}{y}$ if $v(x) \geq v(y) \neq \infty$ and $\mathcal{Q}_0(x, y) = 0$ otherwise while $\mathcal{Q}_1(x, y) := \frac{x}{y}$ if $v(x) > v(y)$ and is zero otherwise.

Remark 2.7. As shown in the work of Denef and van den Dries [9] and Lipshitz and Robinson [15], for example, quantifier elimination for certain valuation rings considered with analytic structure may be obtained in languages possessing \mathcal{Q}_0 and \mathcal{Q}_1 as primitives, but not without these operators.

Definition 2.8. Given a pre-notion of analyticity \mathcal{A} and a first-order language of valuation rings \mathcal{L} as in Remark 2.5, the language $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})$ is the expansion of $\mathcal{L}(\mathcal{A})$ by the function symbol \mathcal{Q}_0 and \mathcal{Q}_1 of domain sort \mathcal{O}^2 and range sorts \mathcal{O} and \mathfrak{m} , respectively. Given a valuation ring with \mathcal{A} -analytic structure there is a natural expansion of the structure to an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})$ -structure.

We recall now the formalism of leading terms and angular components.

Definition 2.9. Let (K, v) be a valued field and $t \in \mathcal{O} = \mathcal{O}_{K,v}$ be a fixed nonzero element of the ring integers of K . For each natural number n , we define the n^{th} leading terms of K relative to K to be the multiplicative monoid $\ell_{n,t}(K) := K/(1 + t^n \mathfrak{m})$. We write $\ell_{n,t}(K)^* := \ell_{n,t}(K) \setminus \{0\}$. We write $r_{n,t}(K) := \mathcal{O}/t^n \mathfrak{m}$. If t is understood we write simply $\ell_n(K)$ for $\ell_{n,t}(K)$ and $r_n(K)$ for $r_{n,t}(K)$. We write $\ell_n: K \rightarrow \ell_n(K)$ for the natural quotient map and $\pi_n: \mathcal{O} \rightarrow r_n(K)$ for the reduction map.

Remark 2.10. While $\ell_n(K)^*$ is naturally a group, it carries additional structure. For instance, the valuation map $v: K \rightarrow \Gamma_K \cup \{\infty\}$ descends to a map on $\ell_n(K)$ which we continue to denote by v . More importantly, addition leaves a trace on $\ell_n(K)$ in the form of a ternary predicate $\tilde{+}_n := \{(x, y, z) \in \ell_n(K)^3 \mid \exists \tilde{x}, \tilde{y}, \tilde{z} \in K \tilde{x} + \tilde{y} = \tilde{z}, \ell_n(\tilde{x}) = x, \ell_n(\tilde{y}) = y, \text{ and } \ell_n(\tilde{z}) = z\}$. In the sequel we shall require that $\ell_n(K)$ remember more structure from K . In particular, we insist that the leading terms remember analytic identities. That is, for each $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})$ -term $f(x_1, \dots, x_m)$ the image of $\{(x_1, \dots, x_m, y) \in K^{m+1} \mid f(\mathbf{x}) = y\}$ under ℓ_n is to be described by an m -ary predicate on ℓ_n .

Remark 2.11. The image of \mathcal{O}^\times in $\ell_n(K)$ may be identified with $r_n(K)^\times$ and the valuation exact sequence $1 \longrightarrow \mathcal{O}^\times \longrightarrow K^\times \xrightarrow{v} \Gamma_K \longrightarrow 0$ descends to $1 \longrightarrow r_n(K)^\times \longrightarrow \ell_n(K)^* \xrightarrow{v} \Gamma_K \longrightarrow 0$.

Remark 2.12. If $t \in \mathcal{O}^\times$ is a unit, then the leading term structures $\ell_{n,t}(K)$ are all identical.

Remark 2.13. In our intended applications we take $t = p$, the residue characteristic, or $t = 1$ when the residue characteristic is zero. In fact, we shall impose this requirement with our axioms.

Remark 2.14. One can consider leading term structures relative to other ideals in \mathcal{O}_K and we shall use $\ell_\infty(K) := K/(1+t^\infty\mathfrak{m})$ where $t^\infty\mathfrak{m} := \{x \in \mathcal{O} \mid (\forall n \in \mathbb{Z}_+) v(x) > v(t^n)\}$. One cannot access $\ell_\infty(K)$ directly in first-order logic, but when the field K is \aleph_1 -compact, $\ell_\infty(K) = \varprojlim \ell_n(K)$ so that it may be approached from first-order data. Note that the ring $\mathcal{O}(K)\left[\frac{1}{t}\right]$ is a valuation ring whose residue field is $r_\infty(K)\left[\frac{1}{\pi_\infty(t)}\right]$. We refer to the corresponding coarsened valuation as v_∞ .

Remark 2.15. In the work of Basarab and Kuhlmann [4], [14], leading term structures are called “additive-multiplicative congruences” or “amc structures.”

Leading term structures already live definably in valued fields, but the way in which they nontrivially combine the value group and certain residue rings can complicate their analysis. By working with angular component functions one can treat these parts separately.

Definition 2.16. An *angular component function of level n* is a section $\text{ac}_n : \ell_n(K)^* \rightarrow r_n(K)^\times$ of the valuation sequence. A *system of angular component functions* is a sequence $\{\text{ac}_n\}_{n=0}^\infty$ where ac_n is an angular component function of level n and these functions commute with the obvious quotient maps between the leading term and residue sorts.

Remark 2.17. As with the leading terms, we shall require that the angular component functions preserve more than just the multiplicative structure.

Remark 2.18. While angular components need not exist in general, they do if (K, v) is sufficiently saturated. Thus, possibly at the cost of replacing (K, v) with an elementarily equivalent structure, we may assume that we have angular component functions.

Let us now fix once and for all a background language \mathcal{L} and theory of valued fields, T_{VF} . We take \mathcal{L} to be a many sorted language having sort symbols VF for the valued field itself, \mathcal{O} for the valuation ring, \mathfrak{m} for the maximal ideal of the valuation ring, Γ for the value group, r_n for the residue rings of Definition 2.9 and r_n^\times for the units in the residue ring, and ℓ_n for the leading terms. The sorts are connected by the inclusion maps $\mathfrak{m} \hookrightarrow \mathcal{O} \hookrightarrow \text{VF}$, $r_n^\times \hookrightarrow r_n$ and $r_n^\times \hookrightarrow \ell_n$, the valuation maps $v : \text{VF} \rightarrow \Gamma$ and $v : \ell_n \rightarrow \Gamma$, the reduction maps $\pi_n : \mathcal{O} \rightarrow r_n$ and $\pi_{m,n} : r_m \rightarrow r_n$, and the leading term maps $\ell_n : \text{VF} \rightarrow \ell_n$ and $\ell_{m,n} : \ell_m \rightarrow \ell_n$. The sorts VF, \mathcal{O} , and r_n come equipped with a copy of the language of rings while Γ is presented in the language of ordered abelian groups and the ℓ_n sorts each have a binary multiplication

operation and a ternary predicate for addition as described above. If we wish to include angular component functions, then expand the language to $\mathcal{L}(\{ac_n\})$.

We axiomatize the theory of valued fields, T_{VF} , in \mathcal{L} with the usual axioms asserting that if $M \models T$, then $\text{VF}(M)$ is a field and that $v: \text{VF}(M) \rightarrow \Gamma(M)$ is a valuation, and that all of the other sorts are interpreted as expected. That is, the inclusion maps $\mathfrak{m}(M) \hookrightarrow \mathcal{O}(M) \hookrightarrow \text{VF}(M)$ are really inclusions and identify their images with the elements of positive valuation and of nonnegative valuation, respectively, the valuation maps are surjective, and the residue ring sorts and leading term sorts really give the residue rings and leading terms, *et cetera*. The one nontrivial point here is that we require $\ell_n(M)$ to be $\text{VF}(M)/(1 + \mathfrak{m}(M))$ ($r_n(M)$ to be $\mathcal{O}(M)/\mathfrak{m}(M)$, respectively) if the residue characteristic is zero and to be $\text{VF}(M)/(1 + p^n \mathfrak{m}(M))$ ($\mathcal{O}(M)/p^n \mathfrak{m}(M)$, respectively) when the residue characteristic is $p > 0$. This condition may be expressed by a set of first-order sentences. Of course, if we work in $\mathcal{L}(\{ac_n\})$, then our theory $T_{VF}(ac)$ expresses that the angular component function symbols are interpreted as angular components.

When we expand to $\mathcal{L}^{\mathcal{Q}}$ our theory $T_{VF}^{\mathcal{Q}}$ includes axioms expressing the definitions of \mathcal{Q}_0 and \mathcal{Q}_1 . Given a pre-notion of analyticity \mathcal{A} , we require of the expanded language $\mathcal{L}(\mathcal{A})$ not only that there be function symbols for the elements on \mathcal{A} but that there be predicates on the leading term sorts corresponding to these functions. Given any \mathcal{L} -theory $T \supseteq T_{VF}$ of valued fields, the theory $T(\mathcal{A})$ is obtained from T by adjoining the axioms expressing that the valuation ring has \mathcal{A} -analytic structure and that the new predicates on the leading terms are interpreted correctly.

Remark 2.19. For the main theorems of this paper we require that the valued fields under consideration have characteristic zero.

We need to say a little about affinoids before finishing the definition of a notion of analyticity. If $M \models T_{VF}(\mathcal{A})$ is a valuation ring with \mathcal{A} -analytic structure and (K', v') is an algebraic extension of $\text{VF}(M)$ with an extension of the valuation v , then there is a unique way to extend the \mathcal{A} -analytic structure to K' . Indeed, it is enough to see this in the case that K' is a finite extension of $\text{VF}(M)$. Fixing a basis for $\mathcal{O}(K')$ over $\mathcal{O}(M)$, one can identify $\mathcal{O}(K')$ with $\mathcal{O}(M)^{[K:\text{VF}(M)]}$. In so doing, one can expand the action of the \mathcal{A} -analytic functions in terms of this basis as well. In particular, if $K' = \text{VF}(M)^{\text{alg}}$ is the algebraic closure of $\text{VF}(M)$, then $(K', v) \models T_{VF}(\mathcal{A})$.

Definition 2.20. Let $M \models T_{VF}(\mathcal{A})$ be a valuation ring with \mathcal{A} -analytic structure and fix an extension v' of v to $K' := \text{VF}(M)^{\text{alg}}$. A S subset of $\mathcal{O}(K')$ is said to be an *affinoid over M* if there are $\gamma_1, \dots, \gamma_n \in \Gamma(M)$ and $a_1, \dots, a_n \in \mathcal{O}(M)$ with $\gamma_1 > \gamma_i$ for $i \neq 1$ and $S = \{z \in \mathcal{O}(K') \mid v(z - a_1) \geq \gamma_1 \wedge \bigwedge_{i=2}^n v(z - a_i) \leq \gamma_i\}$. An affinoid set in M is the intersection of an affinoid set over M with $\mathcal{O}(M)$.

With the background on valued fields in place we are now ready to describe when a pre-notion of analyticity is actually a notion of analyticity.

Definition 2.21. Fix some theory $T \supseteq T_{\text{VF}}$ of valued fields. A *notion of analyticity* (relative to T) is a pre-notion of analyticity, \mathcal{A} , for which Weierstraß division holds uniformly in the following sense. If $M \models T(\mathcal{A})$ and $t(x)$ is an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})_M$ -term in the single \mathcal{O} -variable x , then there are finitely many affinoid subsets F_1, \dots, F_n of $\mathcal{O}(M)$ for which $\mathcal{O}(M) = \bigcup F_i$ and for each i there is a rational function $R_i(X)$ over $\mathcal{O}(M)$ having no poles in F_i and $\mathcal{L}(\mathcal{A})_M$ -terms $E_i(x)$ and $E_i^{-1}(x)$ for which $E_i(x)E_i^{-1}(x) \equiv 1$ on F_i and $t(x) = E_i(x)R_i(x)$ at all but finitely many points of F_i .

Remark 2.22. That the rings of convergent power series over complete DVRs give a notion of analyticity is proven by van den Dries, Haskell and Macpherson in [20]. (Combine Proposition 4.1 with Corollary 3.4 noting that Proposition 4.1 is still general even though it is in Section 4 where the authors claim to specialize to the case of the p -adics.)

Remark 2.23. In our applications, we restrict attention to valued fields of characteristic zero. Thus, the theory T in Definition 2.21 will be T_{VF} together with the set of sentences asserting that the valued field itself has characteristic zero.

Remark 2.24. The condition of uniform Weierstraß division may be expressed more syntactically in that the parameters for the term $t(x)$ may be given as a tuple of variables \mathbf{y} and then the affinoids, the rational functions, and the units $E(x)$ vary uniformly with \mathbf{y} .

If R is any ring and $\sigma : R \rightarrow R$ is an automorphism, then σ extends to an automorphism $\sigma : R[X][[Y]] \rightarrow R[X][[Y]]$ of the power series ring over the polynomial ring over R . For $f \in R[X][[Y]]$ we write the f^σ for the result of applying σ to f .

Definition 2.25. A *notion of difference analyticity* (relative to T as in Definition 2.21), (\mathcal{A}, σ) , is given by a notion of analyticity \mathcal{A} and an automorphism $\sigma : \mathcal{A}_{0,0} \rightarrow \mathcal{A}_{0,0}$ which induces an automorphism on each $\mathcal{A}_{m,n}$.

Definition 2.26. Given a notion of difference analyticity (\mathcal{A}, σ) (relative to T), an \mathcal{A} -analytic difference ring is a model $M \models T(\mathcal{A})$ given together with a distinguished automorphism $\sigma : M \rightarrow M$ which preserves the valuation in the sense that $v(\sigma(x)) = v(x)$ universally and respects the \mathcal{A} -analytic structure in the sense that $\sigma(f(\mathbf{x})) = f^\sigma(\sigma(\mathbf{x}))$ for any \mathcal{A} -function f .

The condition of being an \mathcal{A} -analytic difference ring is clearly axiomatizable in $\mathcal{L}(\mathcal{A}, \sigma)$, the expansion of the language of valuation rings with \mathcal{A} -analytic structure by a symbol for an automorphism.

As in the study of difference algebra, terms in $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma)$ may be expressed using terms from $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})$ applied to prolongations, sequences of the form $\sigma(\mathbf{x}) = (\mathbf{x}, \sigma(\mathbf{x}), \dots, \sigma^n(\mathbf{x}))$. That is, if $t = t(\mathbf{x}) = t(x_1, \dots, x_m)$ is an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma)$ term, then we can find an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})$ term $\tilde{t} = \tilde{t}(x_{0,1}, \dots, x_{0,m}; \dots; x_{n,1}, \dots, x_{n,m})$ so that relative to the theory of \mathcal{A} -analytic difference rings we have $t(\mathbf{x}) = \tilde{t}(\sigma(\mathbf{x}))$. We define the *order* of t to be the least m for which such a \tilde{t} exists. It should be noted that

the order of t when computed in a fixed \mathcal{A} -analytic difference ring may be different from the order when computed relative to the theory of \mathcal{A} -analytic difference rings. In our applications, when we speak of *order* we mean *order relative to a given structure*.

Fix an \mathcal{A} -analytic difference ring M and $A \subseteq M$ a substructure for which $\mathcal{O}(A)$ generates A . If $a \in \mathcal{O}(M)$ and for some $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma)_A$ term $t(x)$ over A we have $t(a) = 0$ but $t(x) \not\equiv 0$ in a neighborhood of a , then we can find such a term of minimal possible order, n , and define the *order of a over A* , $\text{ord}(a/A)$, to be that minimal order. By the uniform Weierstraß division theorem, we may write $t(x)$ as $E(\sigma^n(x))R(\sigma^n(x))$ where R is a rational function over the $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})$ -structure A' generated by A and $a, \dots, \sigma^{n-1}(a)$ having no poles near $\sigma^n(a)$ and E is an $\mathcal{L}(\mathcal{A})$ term over A' which is a unit near $\sigma^n(a)$. Thus, there is actually a nonzero polynomial over A' which vanishes at $\sigma^n(a)$. We define the *degree of a over A* , $\text{deg}(a/A)$, to be the minimal degree, d , of such a polynomial. We combine these data in the pair $(\text{ord}, \text{deg})(a/A) := (\text{ord}(a/A), \text{deg}(a/A))$ and order them lexicographically.

As with pure valued fields and some theories of valued fields with additional structure, the model companions of theories of \mathcal{A} -analytic difference rings are obtained by adjoining variants of Hensel's lemma (and an axiom about the existence of constants) to the theory. Unfortunately, the usual proof of Hensel's lemma breaks down when applied to $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma)$ terms as the quotient operators may introduce discontinuities. However, these terms do define generically continuous functions and if one stays within the correct domain of continuity, Newton approximation techniques do work.

Proposition 2.27. *Suppose that M is an \mathcal{A} -analytic difference ring and let p_0, \dots, p_d be a finite sequence of $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})_M$ terms with parameters from M and variables x_0, \dots, x_{n-1} . Write $P(x) = \sum_{i=0}^d p_i(\sigma(x))(\sigma^n(x))^i$. Abusing notation, we write $P'(x) = \sum_{i=0}^d i p_i(\sigma(x))(\sigma^n(x))^{i-1}$. Assume that $a \in \mathcal{O}(M)$ with $v(P(a)) > 2v(P'(a))$ and that for any $\varepsilon \in \mathcal{O}(M)$ with $v(\varepsilon) \geq v(P(a)) - v(P'(a))$ one has $\ell_0(p_i(a + \varepsilon)) = \ell_0(p_i(a))$ for $i \leq d$. Then there is some $b \in \mathcal{O}(M)$ with $v(b - a) \geq v(P(a)) - v(P'(a))$ and $v(P(b)) > v(P(a))$.*

Proof. A variant of the usual proof applies. Indeed, let $\eta := \sigma^{-n}(\mathcal{Q}_0(-P(a), P'(a)))$ and set $b := a + \eta$. From our hypotheses, $v(a - b) = v(P(a)) - v(P'(a))$ and computing $P(b)$ we have

$$\begin{aligned} P(b) &= \sum_{i=0}^d p_i(a + \eta)(\sigma^n(a + \eta))^i \\ &= \sum_{i=0}^d p_i(a)[1 + \xi_i] \sum_{j=0}^i \binom{i}{j} \sigma^n(a)^{i-j} \sigma^n(\eta)^j \quad \text{where } v(\xi_i) > 0 \\ &\equiv P(a) + P'(a)\sigma^n(\eta) \pmod{P(a)\mathfrak{m}(M)} \\ &\equiv 0 \pmod{P(a)\mathfrak{m}(M)} \quad \square \end{aligned}$$

Corollary 2.28. *With the hypotheses as in Proposition 2.27, there is a maximal pseudoconvergent sequence $\{b_\alpha\}$ from $\mathcal{O}(M)$ with $b_0 = a$ and $v(P(b_\alpha))$ increasing*

with α . If in addition $\mathcal{O}(M)$ is maximally complete, then $b := \lim b_\alpha$ exists and $P(b) = 0$.

We convert the last part of this corollary into our version of henselianity for \mathcal{A} -analytic difference rings.

Definition 2.29. We say that the \mathcal{A} -analytic difference ring M is \mathcal{A} -analytically difference henselian if the conclusion of Corollary 2.28 holds for M . That is, given a sequence of $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})_M$ terms p_0, \dots, p_d with variables x_0, \dots, x_{n-1} writing $P(x) = \sum p_i(\sigma(x), \mathbf{a})\sigma^n(x)^i$ if $a \in \mathcal{O}(M)$ has the property that $v(P(a)) > 2v(P'(a))$ while for any $\varepsilon \in \mathcal{O}(M)$ with $v(\varepsilon) \geq v(P(a)) - v(P'(a))$ we have $\ell_0(p_i(\sigma(a))) = \ell_0(p_i(\sigma(a + \varepsilon)))$ for $i \leq d$, then there is some $b \in \mathcal{O}(M)$ with $P(b) = 0$ and $v(b - a) \geq v(P(a)) - v(P'(a))$.

Remark 2.30. It should be noted that even when there are no quotient operators, and even in the case of difference polynomials, the continuity hypothesis is nontrivial.

Visibly, the condition of being \mathcal{A} -analytically difference henselian is first-order expressible. In axiomatizing the theory of \mathcal{A} -analytically difference henselian rings, $T_{\mathcal{A}\text{-DH}}$, we impose two additional requirements beyond those of Definition 2.29. First, we insist that every model of $T_{\mathcal{A}\text{-DH}}$ be of characteristic zero. Secondly, we demand that the valued field have enough constants in the sense that for every element of the value group there is some element of the field fixed by σ and having that valuation. This last condition can be ostensibly weakened by requiring the existence of σ -fixed elements of each valuation only at the level of the leading terms. For the remainder of this paper, when we speak of an \mathcal{A} -analytically difference henselian ring we mean a model of $T_{\mathcal{A}\text{-DH}}$ where (\mathcal{A}, σ) is some notion of difference analyticity.

3. AKE theorems for analytically difference henselian rings

In this section we state and prove our main relative completeness and quantifier elimination theorems for \mathcal{A} -analytically difference henselian rings. As with much of the earlier work on pure valued fields and on algebraic valued difference and differential fields (but, remarkably, unlike most previous work on the model theory of analytic functions on valued fields) we prove our results by employing a model theoretic test for completeness and quantifier elimination involving extensions of partial isomorphisms.

Simply put, our theorem is that for a fixed notion of difference analyticity, (\mathcal{A}, σ) , the theory $T_{\mathcal{A}\text{-DH}}$ of \mathcal{A} -analytically difference henselian rings is complete and eliminates quantifiers relative to the leading term sorts, and even, resplendently so. As we expect the meaning here of relativity and resplendence may require some explanation, we describe these terms now before announcing our theorem in its official formulation.

Given a many sorted language \mathcal{L} and a nonempty set Σ of \mathcal{L} -sort symbols, the restriction of \mathcal{L} to Σ , $(\mathcal{L} \upharpoonright \Sigma)$, is the language having sort symbols Σ and as basic function, relation, and constant symbols exactly those from \mathcal{L} which refer only to sorts in Σ . That is, a function symbol f of \mathcal{L} is a function symbol of $(\mathcal{L} \upharpoonright \Sigma)$ just in case its domain sort is a sequence of sorts from Σ and its range sort belongs to Σ while a relation symbol of \mathcal{L} belongs to the restricted language if its field sort is a sequence of elements of Σ and an \mathcal{L} -constant symbol is an $(\mathcal{L} \upharpoonright \Sigma)$ -constant if its sort belongs to Σ . If M is an \mathcal{L} -structure, then the restriction of M to Σ is simply the $(\mathcal{L} \upharpoonright \Sigma)$ -structure $(M \upharpoonright \Sigma)$ consisting of the M -interpretation of the sorts in Σ and the nonlogical $(\mathcal{L} \upharpoonright \Sigma)$ -symbols.

Definition 3.1. Given a many sorted language \mathcal{L} and a nonempty set Σ of \mathcal{L} -sort symbols we say that the \mathcal{L} -theory T is *complete relative to Σ* if for any model $M \models T$ the theory $T \cup \text{Th}_{(\mathcal{L} \upharpoonright \Sigma)}(M \upharpoonright \Sigma)$ is complete.

To discuss relative quantifier elimination we need to recall Morleyization. Given a language \mathcal{L} , the Morleyization \mathcal{L}^{Mor} of \mathcal{L} is obtained by adjoining to \mathcal{L} a new relation symbol $R_\phi(x_1, \dots, x_n)$ for each \mathcal{L} -formula ϕ with the free variables x_1, \dots, x_n . The \mathcal{L}^{Mor} -theory $T_{\mathcal{L}}^{\text{Mor}}$ is defined by

$$T_{\mathcal{L}}^{\text{Mor}} := \{\forall x_1 \cdots \forall x_n (R_\phi(\mathbf{x}) \leftrightarrow \phi(\mathbf{x})) \mid \phi \text{ an } \mathcal{L}\text{-formula}\}$$

On general grounds, any extension of $T_{\mathcal{L}}^{\text{Mor}}$ in \mathcal{L}^{Mor} eliminates quantifiers.

Definition 3.2. Given a many sorted language \mathcal{L} and a nonempty set Σ of \mathcal{L} -sort symbols we say that the \mathcal{L} -theory T *eliminates quantifiers relative to Σ* if the theory $T \cup T_{(\mathcal{L} \upharpoonright \Sigma)}^{\text{Mor}}$ eliminates quantifiers in $\mathcal{L} \cup (\mathcal{L} \upharpoonright \Sigma)^{\text{Mor}}$.

We mentioned that our theorems hold resplendently. We employ this enhancement of the theorem when discussing angular components. Essentially, by resplendent relative completeness (respectively, resplendent relative quantifier elimination) we mean that relative completeness (respectively, relative quantifier elimination) continues to hold even after arbitrarily enriching the sorts to which we relativize.

Definition 3.3. Let \mathcal{L} be a many sorted language and Σ a nonempty set of \mathcal{L} -sort symbols. We say that the \mathcal{L} -theory T is *resplendently complete relative to Σ* (respectively, *resplendently eliminates quantifiers relative to Σ*) if for any expansion $\mathcal{L}' \supseteq (\mathcal{L} \upharpoonright \Sigma)$ having only Σ as sort symbols and any \mathcal{L}' -theory T' the theory $T \cup T'$ is complete relative to Σ (respectively, eliminates quantifiers relative to Σ).

With this general nonsense on many sorted languages in place we may now state our main theorem.

Theorem 3.4. *The theory $T_{\mathcal{A}\text{-DH}}$ of \mathcal{A} -analytically difference henselian rings is resplendently complete relative to the leading terms sorts and resplendently eliminates quantifiers relative to the leading terms.*

Using general results on the existence of angular components, we deduce a stronger relative completeness theorem from Theorem 3.4.

Theorem 3.5. *The theory $T_{\mathcal{A}\text{-DH}}$ of \mathcal{A} -analytically difference henselian rings is complete relative to the value group and residue ring sorts.*

As a particular application of Theorem 3.5 we see that if $k \hookrightarrow k'$ is an extension of algebraically closed fields of characteristic p , then the corresponding extension of rings of Witt vectors, $W[k] \hookrightarrow W[k']$, is elementary in the language $\mathcal{L}(\mathcal{A}, \sigma)$ where $\mathcal{A}_{m,n} = W[k][X][[Y]]$ and σ is interpreted as the Witt–Frobenius. We shall expand on this observation and exploit it in Section 4.

As is our wont, we shall prove Theorem 3.4 by converting it into a statement about extending isomorphisms and then actually proving the statement on extensions by considering the cases of residue field, totally ramified, and immediate extensions separately. Some of these steps require merely routine modifications to the proofs in the algebraic setting, but others are considerably trickier.

The reader should consult Section 7 of [17] or Theorem 8.4.1 of [11] for a discussion of why the following technical theorem is equivalent to Theorem 3.4.

Theorem 3.6. *Let \mathcal{L}' be an expansion of the restriction of $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma)$ to the leading term sorts, $(\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma) \upharpoonright \text{LT})$, having no new sort symbols. Suppose that M_1 and M_2 are two saturated \mathcal{A} -analytically difference henselian rings each of the same cardinality $> (|\mathcal{L}'|^{\aleph_0})^+$ considered in the language $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma) \cup \mathcal{L}'^{\text{Mor}}$. Suppose moreover that $(M_1 \upharpoonright \text{LT}) \equiv_{\mathcal{L}'} (M_2 \upharpoonright \text{LT}) \models T_{\mathcal{L}'}$. Suppose that $A_1 \subseteq M_1$ and $A_2 \subseteq M_2$ are two small (of cardinality at most $|\mathcal{L}'|$) substructures of M_1 and M_2 for which $\mathcal{O}(A_i)$ generates A_i and that $f: A_1 \rightarrow A_2$ is an isomorphism of $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma) \cup (\mathcal{L}')^{\text{Mor}}$ -structures. If $a \in \mathcal{O}(M_1)$ is any element, then there is an extension of f to an isomorphism between the substructure of M_1 generated by A_1 and a , $A_1 \langle a \rangle$, and a substructure of M_2 .*

Throughout the remainder of this section we concentrate on proving Theorem 3.6, and, hence, also Theorem 3.4. In the course of this proof we shall reduce the problem to other statements with stronger hypotheses. As these restrictions are established, we shall display our new hypotheses as boxed statements.

As M_1 and M_2 are saturated of the same cardinality and $(M_1 \upharpoonright \text{LT})$ and $(M_2 \upharpoonright \text{LT})$ are elementarily equivalent, they are actually isomorphic. Since the map $f: A_1 \rightarrow A_2$ is an isomorphism of $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma) \cup (\mathcal{L}')^{\text{Mor}}$ -structures, and, each $(M_i \upharpoonright \text{LT})$ eliminates quantifiers, the restrictions of these structures to the leading terms are actually isomorphic over f . Let us fix such an isomorphism $\tilde{f}: (M_1 \upharpoonright \text{LT}) \rightarrow (M_2 \upharpoonright \text{LT})$ and thereby arrive at our first reduction.

$\tilde{f} \cup f: A_1 \cup (M_1 \upharpoonright \text{LT}) \rightarrow A_2 \cup (M_2 \upharpoonright \text{LT})$ is an isomorphism of $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma) \cup (\mathcal{L}')^{\text{Mor}}$ -structures.

We fix now $N_1 \preceq M_1$ and $N_2 \preceq M_2$ two $|\mathcal{L}'|^+$ -compact elementary substructures each of cardinality less than that of M_1 for which $A_1 \langle a \rangle \subseteq N_1$ and $A_2 \subseteq N_2$. Our hypotheses on the saturation of M_1 and M_2 and on their cardinalities ensure that such structures exist. In the course of our construction of an extension of f we shall initially extend inside N_1 taking values in N_2 until N_i is an immediate extension of A_i and then we extend f to a maximal immediate extension of N_1 inside M_1 .

With the next lemma we show that the map f may be extended so as to add new elements to the residue ring $r_\infty(A_1)$.

Lemma 3.7. *Let $a \in r_\infty(N_1)$. Suppose that $(\text{ord}, \text{deg})(a/r_\infty(A_1)) = (m, d)$. Let $\tilde{p}_0, \dots, \tilde{p}_d$ be $\mathcal{L}^\Omega(\mathcal{A})_{A_1}$ terms in the variables x_0, \dots, x_{n-1} for which the reductions under π_∞ , $p_i = \pi_\infty(\tilde{p}_i)$, give well-defined functions at $(a, \sigma(a), \dots, \sigma^{m-1}(a))$ and $P(a) = \sum p_i(\sigma(a))(\sigma^m(a))^i = 0$. Let $\tilde{P} = \sum \tilde{p}_i(\sigma(x))(\sigma^m(x))^i$. Then there are elements $\tilde{a} \in \mathcal{O}(N_1)$ and $\tilde{b} \in \mathcal{O}(N_2)$ for which $\tilde{P}(\tilde{a}) = 0$, $\tilde{P}^f(\tilde{b}) = 0$, $\pi_\infty(\tilde{a}) = a$, $\tilde{f}(a) = \pi_\infty(\tilde{b})$, and f extends to an isomorphism defined on the structure $A_1 \langle \tilde{a} \rangle$ which has no new elements in its value group taking \tilde{a} to \tilde{b} .*

Proof. Let $a' \in \mathcal{O}(N_1)$ be any lifting of a . By our minimality assumption, $P'(a) \neq 0$. As $P(a) = 0$ in $r_\infty(N_1)$, we see that, $2v(\tilde{P}'(a')) < v(\tilde{P}(a'))$. Moreover, because the terms $p_i(\sigma(x))$ are well-defined at a , their leading terms do not depend on the choice of a' . Hence, as N_1 is \mathcal{A} -analytically difference henselian, there is some \tilde{a} lifting a and satisfying $\tilde{P}(\tilde{a}) = 0$. Likewise, using \aleph_1 -compactness of N_2 we can find $\tilde{b} \in \mathcal{O}(N_2)$ with $\tilde{P}^f(\tilde{b}) = 0$ and $\pi_\infty(\tilde{b}) = \tilde{f}(a)$.

We argue by induction on $n \leq m$ that if Q is a term of order n , then $\tilde{f}(\ell_\infty(Q(\tilde{a}))) = \ell_\infty(Q^f(\tilde{b}))$. By the uniform Weierstraß property, we may express Q near \tilde{a} as $E(\sigma^n(\tilde{a}))R(\sigma^n(\tilde{a}))$ where E is given by an $\mathcal{L}(\mathcal{A})$ term over the $\mathcal{L}^\Omega(\mathcal{A})$ -structure generated by A_1 and $\tilde{a}, \dots, \sigma^{n-1}(\tilde{a})$ and is a unit near $\sigma^n(\tilde{a})$ and R is a rational function over the same structure having no poles near $\sigma^n(\tilde{a})$. In the case that $n = m$, we may assume that the degrees of the numerator and denominator of R are less than d . By induction, the ∞ -leading terms of the parameters for E and R are under control. As the quotient operators are not applied to $\sigma^n(\tilde{a})$ in E and E is a unit near $\sigma^n(\tilde{a})$, its ∞ -leading term is determined by that of $\sigma^n(\tilde{a})$. Write $R(\sigma^n(\tilde{a})) = S(\sigma^n(\tilde{a}))/T(\sigma^n(\tilde{a}))$ where S and T are polynomials. Write $S = c\tilde{S}$ where $v(c)$ is equal to the Gauß valuation of S . Then $\pi_\infty \tilde{S}$ gives a nonvanishing polynomial at $\sigma^n(\tilde{a})$ as either $n < \text{ord}(a/r_\infty(A_1))$ or $\text{deg } \pi_\infty(\tilde{S}) < \text{deg}(a/r_\infty(A_1))$. Thus, $\ell_\infty(\tilde{S}(\tilde{a})) = \pi_\infty(\tilde{S})(a)$. Applying the same reasoning to T , we conclude the induction and, hence, also the proof of this lemma. \square

Repeatedly applying Lemma 3.7 we can extend f so that $r_\infty(A_i) = r_\infty(N_i)$. However, we delay doing this until we have achieved $\Gamma(A_i) = \Gamma(N_i)$.

With the following steps we enlarge the value group of A_1 . Before actually adding new elements to the value group, we extend f so that its domain has enough constants.

Lemma 3.8. *If $c \in \mathcal{O}(A_1)$, then f extends to some $A_1 \langle \varepsilon \rangle \subseteq N_1$ where $v(\varepsilon) = v(c)$, $\sigma(\varepsilon) = \varepsilon$, and $\Gamma(A_1) = \Gamma(A_1 \langle \varepsilon \rangle)$.*

Proof. Take $\zeta \in \mathcal{O}(N_1)$ with $\sigma(\zeta) = \zeta$ and $v(\zeta) = v(c)$. Such an element exists by our axiom that \mathcal{A} -analytically difference henselian rings have enough constants. Set $\eta := \mathcal{Q}_0(\varepsilon, c)$. Then η is a nonzero solution to the linear difference equation $\sigma(X) - \mathcal{Q}(c, \sigma(c))X = 0$, even upon reduction to $r_\infty(N_1)$. Thus, there are infinitely many solutions to $\sigma(X) - \pi_\infty(\mathcal{Q}(c, \sigma(c)))X = 0$ in $r_\infty(N_1)$ and by $|\mathcal{L}'|^+$ -compactness, at least $|\mathcal{L}'|^+$ many solutions. In particular, there some solution a which is not algebraic over $r_\infty(A_1)$. Let \tilde{a} and \tilde{b} be given by Lemma 3.7 applied to $\tilde{P}(X) = \sigma(X) - \pi_\infty(\mathcal{Q}(c, \sigma(c)))$. Set $\varepsilon := \tilde{a} \cdot c$. \square

Iterating this construction so as to consider all the elements of the value group of A_1 , we may suppose that A_1 and A_2 have enough constants.

A_1 and A_2 have enough constants

For purely ramified extensions we consider the cases of algebraic and transcendental extensions separately.

Lemma 3.9. *If $\varepsilon \in \mathcal{O}(N_1)$, $\sigma(\varepsilon) = \varepsilon$, $\varepsilon^n =: \zeta \in \mathcal{O}(A_1)$, and $mv(\varepsilon) \notin \Gamma(A_1)$ for $m < n$, then f extends to $A_1\langle\varepsilon\rangle$.*

Proof. That there is some $\eta \in N_2$ fixed by σ with $\eta^n = f(\zeta)$ and that the map extending f sending ε to η preserves the valued difference structure is already known from the algebraic case. As noted in Section 2, the \mathcal{A} -analytic structure extends uniquely to algebraic extensions. \square

We extend now to transcendental expansions of the value group.

Lemma 3.10. *If $\varepsilon \in \mathcal{O}(N_1)$ is fixed by σ and $nv(\varepsilon) \notin \Gamma(A_1)$ for all $n \in \mathbb{Z}_+$, then there is some $\eta \in \mathcal{O}(N_2)$ also fixed by σ with $\tilde{f}(\ell_\infty(\varepsilon)) = \ell_\infty(\eta)$ for which f extends to $A_1\langle\varepsilon\rangle$ via $\varepsilon \mapsto \eta$.*

Proof. Let $\zeta \in \mathcal{O}(N_2)$ be any element with $\ell_\infty(\zeta) = \tilde{f}(\ell_\infty(\varepsilon))$ and let $P(X) = \sigma(X) - X$. Then $v(P(\zeta)) > v(\zeta) > 0 = v(P'(\zeta))$ as the leading term of ζ is a constant. Indeed, we even have $v_\infty(P(\zeta)) > v_\infty(\zeta)$ where v_∞ is the coarsened valuation. It follows that if $\xi \in \mathcal{O}(N_2)$ with $v(\xi) \geq v(P(\zeta))$, then $\ell_\infty(-(\zeta + \xi)) = \ell_\infty(-\zeta)$. Hence, our version of Hensel's lemma applies and we can find some $\eta \in \mathcal{O}(N_2)$ with $\ell_\infty(\eta) = \ell_\infty(\zeta) = \tilde{f}(\ell_\infty(\varepsilon))$ and $\sigma(\eta) = \eta$.

Since $\sigma(\varepsilon) = \varepsilon$, every element of $\mathcal{O}(A_1\langle\varepsilon\rangle)$ can be expressed as an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})_{A_1}$ term applied to ε . Likewise, the same is true of η with A_1 replaced by A_2 . So, it suffices to show that if $t(x)$ is an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})_{A_1}$ term, then $\tilde{f}(\ell_\infty(t(\varepsilon))) = \ell_\infty(t^f(\eta))$.

Using uniform Weierstraß division to express $t(x)$ as $E(x)R(x)$ where E is an $\mathcal{L}(\mathcal{A})_{A_1}$ term which is a unit near ε and $R(x)$ is a rational function over $\mathcal{O}(A_1)$, we see that $\ell_\infty(E(\varepsilon))$ depends just on $\ell_\infty(\varepsilon)$ and if $R(x) = (\sum a_i x^i) / (\sum b_j x^j)$, then $\ell_\infty(R(\varepsilon)) = \ell_\infty(a_{i_0})\ell_\infty(\varepsilon)^{i_0-j_0} \ell_\infty(b_{j_0})$ where $v(a_{i_0}) + i_0 v(\varepsilon) = \min_i v(a_i) + i v(\varepsilon)$ and $v(b_{j_0}) + j_0 v(\varepsilon) = \min_j v(b_j) + j v(\varepsilon)$. \square

Applying Lemmata 3.9 and 3.10 repeatedly, alternating the rôles of N_1 and N_2 , we may extend f so that $\Gamma(A_i) = \Gamma(N_i)$ for $i \in \{0, 1\}$. Once this has been achieved, we may apply Lemma 3.7 repeatedly to extend f so that N_i is an immediate extension of A_i .

Let us state this result as our second reduction.

N_i is an immediate extension of A_i for $i \in \{0, 1\}$

Fix now \widehat{N}_1 a maximal immediate extension of N_1 in M_1 and a maximal immediate extension \widehat{N}_2 of N_2 in M_2 . We shall actually extend f to \widehat{N}_1 .

Working by induction in \widehat{N}_1 we may assume that a has the least possible (ord, deg) over A_1 of new elements of N_1 . That is:

If $b \in \mathcal{O}(N_1)$ and $(\text{ord}, \text{deg})(b/A_1) < (n, d) := (\text{ord}, \text{deg})(a/A_1)$,
then $b \in \mathcal{O}(A_1)$.

Working by induction further we may assume that whenever we have a pseudoconvergent solution to a low (ord, deg) \mathcal{A} -analytic difference equation over A_1 in N_1 , then we have an actual solution.

If $Q(x) = \sum_{i=0}^e q_i(x, \sigma(x), \dots, \sigma^{m-1}(x))(\sigma^m(x))^i$ where $(m, e) < (n, d)$ and each q_i is an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})_{A_1}$ term and $\{x_\alpha\}$ is a pseudosolution to Q in the sense that $v(Q(x_\alpha))$ is increasing with α and Hensel's lemma applies at each α , then there is some $b \in \mathcal{O}(\widehat{N}_1)$ with x_α pseudoconverging to b and $Q(b) = 0$.

We fix now a maximal pseudoconvergent approximation $\{x_\alpha\}$ to a from $\mathcal{O}(A_1)$ and $P(X) = \sum_{i=0}^d p_i(\sigma(X))(\sigma^n(X))^i$ a minimal equation for a over A_1 . We shall show the following.

1. For Q of lower complexity than that of P (that is, Q is a polynomial in $\sigma^n(X)$ of degree less than d having coefficients which are $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma)_{A_1}$ terms of order less than n) we have $\ell_\infty(Q(a)) = \ell_\infty(Q(x_\alpha))$ for $\alpha \gg 0$.
2. Indeed, we shall show that $v_\infty(Q(a) - Q(x_\alpha)) > v(Q(a)) + v(a - x_\alpha)$ for $\alpha \gg 0$.
3. Possibly replacing P with a refinement, Hensel's lemma applies along $\{x_\alpha\}$.
4. There is some $b \in M_2$ for which $\{f(x_\alpha)\}$ is a pseudoconvergent approximation and $P(b) = 0$.

It follows that we may extend f by sending a to b and that our inductive stipulations on f and \widehat{N}_1 continue to hold.

We work by induction on $m = \text{ord}(Q)$ to prove the first of these points.

We observe first that if U is an $\mathcal{L}^{\mathcal{Q}}(\mathcal{A}, \sigma)_{A_1}$ term of order less than m , then for $\alpha \gg 0$ we have $v(a - x_\alpha) > v(\sigma^m(a) - U(a))$. Indeed, take α large enough so that the valuation inequality stated in Part 2 above holds for U . Assuming that

$v(\sigma^m(a) - U(a)) \geq v(a - x_\alpha) = v(\sigma^m(x_\alpha - a))$, then we have $v(\sigma^m(x_\alpha) - U(x_\alpha)) = v((\sigma^m(a) - U(a)) + (\sigma^m(x_\alpha - a)) + (U(x_\alpha) - U(a))) \geq v(a - x_\alpha)$. Hensel's lemma then applies to produce some y_α with $\sigma^m(y_\alpha) = U(y_\alpha)$ and $v(y_\alpha - x_\alpha) \geq v(a - x_\alpha)$. But then by the boxed reduction above, the sequence $\{y_\alpha\}$, and hence also $\{x_\alpha\}$ has a pseudolimit in \widehat{N}_1 contradicting its maximality.

The point of this observation is that any affinoid defined over the $\mathcal{L}^{\mathcal{Q}}(\mathcal{A})$ -structure generated by A_1 and $a, \dots, \sigma^{m-1}(a)$ containing $\sigma^m(a)$ also contains points of the form $\sigma^m(x_\alpha)$.

Near $\sigma^m(a)$ we can write

$$\mathcal{Q}(x) = E(a, \dots, \sigma^{m-1}(a); \sigma^m(x))R(a, \dots, \sigma^{m-1}(a); \sigma^m(x))$$

where the quotient operators are not applied to $\sigma^m(x)$ in E and E is a unit near a and R is a rational function in $\sigma^m(x)$ with no poles near $\sigma^m(a)$. By induction, the parameters in E and R have the same ∞ -leading terms if $(a, \dots, \sigma^{m-1}(a))$ is replaced by $(x_\alpha, \dots, \sigma^{m-1}(x_\alpha))$ for $\alpha \gg 0$.

Since $\ell_\infty(x_\alpha) = \ell_\infty(a)$, E is a unit, and the ∞ -leading terms of the coefficients of $E(x_\alpha, \dots, \sigma^{m-1}(x_\alpha); X)$ and $E(a, \dots, \sigma^{m-1}(a); X)$ are the same, it follows that $\ell_\infty(E(\sigma(a))) = \ell_\infty(E(\sigma(x_\alpha)))$. Moreover, since the quotient operator is not applied to the last variable and $v(E(\sigma(x_\alpha))) = 0$, the usual Taylor series expansion can be used to see that $v(E(\sigma(x_\alpha)) - E(\sigma(a))) = \gamma + Nv(x_\alpha - a)$ for some fixed $\gamma \in v(\mathcal{O}(A_1))$.

We can write R as $U(x_0, \dots, x_m)/V(x_0, \dots, x_m)$ where each of U and V is a polynomial in x_m . Let us write $U = \sum u_i(x_0, \dots, x_{m-1})x_m^i$. By induction we know, among other things, that $\ell_\infty(u_i(\sigma(a))) = \ell_\infty(u_i(\sigma(x_\alpha)))$ for all i and $\alpha \gg 0$. Replacing U with $\mathcal{Q}(U, c)$ where $c \in \mathcal{O}(A_1)$ and $v(c) = \min_i v(u_i(\sigma(a)))$ we may assume that $v(u_i(\sigma(a))) = 0$ for some i .

Write $x_\alpha = a + y_\alpha$.

Let us expand $U(x_\alpha)$.

$$\begin{aligned} U(x_\alpha) &= \sum u_i(\sigma(a + y_\alpha))(\sigma^m(a + y_\alpha))^i \\ &= \sum_{i,j} u_i(\sigma(a))[1 + \xi_i] \binom{i}{j} \sigma^m(a)^{i-j} \sigma^m(y_\alpha)^j \quad \text{where } v_\infty(\xi_i) > 0 \\ &= \sum_j [1 + \zeta_j] \frac{1}{j!} U^{(j)}(a) \sigma^m(y_\alpha)^j \quad \text{where } v_\infty(\zeta_j) > 0. \end{aligned}$$

For $\alpha \gg 0$, the summands on the righthand side of the equation all have different v_∞ valuations. Thus, $\ell_\infty(U(x_\alpha)) = \ell_\infty(\frac{1}{j!} U^{(j)}(a) \sigma^m(y_\alpha)^j)$ for the j which minimizes the valuation of the expression on the right. If this j is zero, then we are done. As we have reduced to the case that $v(u_i(\sigma(a))) = 0$ for some i , it follows that the j for which the valuation is minimized must have $v_\infty(U^{(j)}(a)) = 0$. Writing $j = k + 1$, we see that Hensel's lemma applies to $U^{(k)}(X)$ along x_α so that by our inductive hypothesis the sequence x_α pseudoconverges to a solution to $U^{(k)}(x) = 0$ contradicting its maximality. Hence, $\ell_\infty(U(a)) = \ell_\infty(U(x_\alpha))$.

Repeating this calculation with V in place of U , we finish the proof of points 1. and 2.

The above calculations apply as well to the case that $U = P$. This time since $P(a) = 0$, necessarily the minimal valuation of a summand on the right is obtained for some $j > 0$. If this j is not one and even if $v_\infty(P'(a)) \neq 0$, then as above x_α pseudoconverges to a solution of some derivative of P . Thus, Hensel's lemma applies to P along x_α and we can find the requisite solution to $P^f(X) = 0$ in $\mathcal{O}(M_2)$.

Conversely, the above calculations show that if we assumed merely that $a \in \mathcal{O}(M_1)$, then there is an immediate extension of \widehat{N}_1 in which x_α pseudoconverges to a solution to $P(X) = 0$. Indeed, arguing by induction on $(\text{ord}, \text{deg})(a/\widehat{N}_1)$ we may assume that P is also a minimal equation for a over \widehat{N}_1 . With the above calculations we never invoked the fact that a lives in an immediate extension of A_1 . Therefore, $\ell_\infty(Q(a)) = \ell_\infty(Q(x_\alpha)) \in \ell_\infty(A_1)$ for each lower complexity Q .

With these observations we conclude the proof of Theorem 3.6.

4. Model theory of p -differential geometry

In this section we apply the results from Section 3 to the theory of p -differential functions obtaining amongst other theorems a uniform version of the Manin–Mumford conjecture over $W[\mathbb{F}_p^{\text{alg}}]$.

Before discussing applications to p -differential functions we verify that the Witt vectors may indeed be regarded as \mathcal{A} -analytic difference henselian rings.

The reader may wish to consult Section 17 of [10] for more details on the Witt vectors. Recall that there is a functor W taking a perfect field k of characteristic $p > 0$ and returning a complete valuation ring $W[k]$ whose maximal ideal is generated by p and whose residue field is naturally isomorphic to k . From the functoriality of the Witt vector construction it follows that the Frobenius automorphism $\tau: k \rightarrow k$ induces an automorphism $W(\tau): W[k] \rightarrow W[k]$ which reduces to τ modulo p . We refer to $W(\tau)$ as the *Witt–Frobenius*. It follows from the construction of $W(\tau)$ that it preserves the p -adic valuation on $W[k]$.

There is more than one reasonable choice for the analytic structure on $W[k]$. If we fix k , then we may wish to take $\mathcal{A}_{m,n} := W[k][X][[Y]]$. In this way we recover the rings of convergent power series by specializing the variables ranging over the maximal ideal. If we wish to work uniformly in p , then we may prefer to use $\mathbb{Z}[X][[Y]]$. In any case, the uniform Weierstraß division property follows from the main results of [20].

The most natural angular component structure on the Witt vectors is defined by taking the powers of p as the constant representatives of the value group. Henceforth, when we consider the Witt vectors with angular components we insist upon this choice. Fixing a choice of \mathcal{A} as in the previous paragraph, we find now that the theory of $W[k]$ in $\mathcal{L}^Q(\mathcal{A}, \sigma, \text{ac})$ is determined by the theory of k and admits quantifier

elimination relative to k and the value group. From Theorem 3.4 we require the theories of all of the residue rings to determine the full theory of the \mathcal{A} -analytic difference henselian ring. In the case of the Witt vectors, the intermediate quotients $r_n(W[k]) = W[k]/p^{n+1}W[k]$ are uniformly interpretable as the k -rational points of ring schemes over k . Thus, their theories and questions about quantifier elimination for these rings are determined by k .

Let us note two consequences of this characterization of the theory of the Witt vectors as an \mathcal{A} -analytic difference ring. First, if $k \hookrightarrow k'$ is an elementary extension of perfect fields, then $W[k] \hookrightarrow W[k']$ is also elementary. Secondly, the residue field is orthogonal to the value group in the sense that if $X \subseteq r_0(W[k])^n \times \Gamma(W[k])^m$ is any definable set, then X is a finite Boolean combination of sets of the form $Y \times Z$ where $Y \subseteq k^n$ is definable in k and $Z \subseteq \mathbb{Z}^m$ is definable in $(\mathbb{Z}, +, 0, <)$.

Let us turn now to a model theoretic study of p -differential geometry. As we noted in the introduction, if $\sigma : W[k] \rightarrow W[k]$ is the Witt–Frobenius, then the operator $\delta : W[k] \rightarrow W[k]$ defined by $\delta(x) := \frac{1}{p}(\sigma(x) - x^p)$ is a p -derivation and the functions of the form $f(\mathbf{x}) = F(\mathbf{x}, \delta\mathbf{x}, \dots, \delta^m\mathbf{x})$ where $\mathbf{x} = (x_1, \dots, x_n)$ and F is given by a convergent power series in $n(m+1)$ variables are the p -differential functions on $W[k]^n$. We concentrate on one class of p -differential functions constructed by Buium, namely the p -differential characters on abelian varieties.

As an illustration of the method, we prove a uniform version of the Manin–Mumford conjecture for abelian varieties over $W[k]$. Recall that the Manin–Mumford conjecture (or Raynaud’s theorem [16]) asserts that if A is an abelian variety over an algebraically closed field K of characteristic zero and $X \subseteq A$ is a closed subvariety, then the intersection of $X(K)$ with the torsion subgroup of $A(K)$ is a finite union of translates of the torsion subgroups of group subvarieties of A . For the purposes of giving this theorem a more quantitative form it can help to present it in terms of the Ueno locus of X .

Recall that the Ueno locus of X , $\text{Ueno}(X)$, is the subvariety of X defined by $x \in \text{Ueno}(X)(K)$ if and only if there is an abelian subvariety $B \leq A$ for which $x + B \subseteq X$. We shall have occasion to use the fact, noted in [13], that if the variety X varies in an algebraic family, then so does $\text{Ueno}(X)$. The Manin–Mumford conjecture implies that there are only finitely many torsion points in $X(K)$ which do not lie in $\text{Ueno}(X)(K)$. In fact, if one establishes this finiteness result for the number of torsion points lying on varieties outside their Ueno loci, then the Manin–Mumford statement follows formally.

With our terms defined we can state our uniform version of the Manin–Mumford conjecture.

Theorem 4.1. *Let k be an algebraically closed field of characteristic $p > 2$, S a variety (reduced, integral scheme of finite type) over $W[k]$ and $A \rightarrow S$ an abelian scheme over S . Let $X \subseteq A$ be a closed subscheme. Then there is a natural number N such that for any point $s \in S(W[k])$ the number of torsion points in $A_s(W[k])$ lying in $X_s(W[k])$ but outside of $\text{Ueno}(X_s)(W[k])$ is bounded by N .*

Remark 4.2. The restriction to odd p is an artifact of our proof in that this is an hypothesis for the published theorem of Buium on the existence of p -differential characters.

Remark 4.3. Theorem 4.1 is similar to the main theorem of [18] but is incomparable in terms of its strength. The result in [18] is weaker in that one requires $A \rightarrow S$ to be a universal abelian variety over a moduli space and one obtains information only about fibres which are canonical lifts, but it is stronger in the sense that Zariski closure of the intersection of $X(W[k])$ with the set of torsion points on canonical lift fibres is described with greater precision than is possible under the hypotheses of Theorem 4.1.

As with some of the other model theoretic theorems describing the intersection of subvarieties of abelian varieties with certain special subgroups, we study intersections of varieties with certain uniformly definable groups containing the torsion groups in lieu of directly analyzing the torsion groups themselves. Unlike some of the other work, rather than offering an alternative proof of the Manin–Mumford conjecture itself, we use Raynaud’s theorem to derive this uniform version.

Before recalling Buium’s construction of p -differential characters on abelian varieties we highlight the crucial features of the groups obtained as the kernels of his characters that we shall exploit.

Definition 4.4. Let k be an algebraically closed field of characteristic $p > 0$. If X is a scheme over $W[k]$ and n is a natural number, then we write $\rho_n: X(W[k]) \rightarrow X(W[k]/p^{n+1}W[k])$ for the reduction modulo p^{n+1} map. If $n < m$, then we write $\rho_{m,n}: X(W[k]/p^{m+1}W[k]) \rightarrow X(W[k]/p^{n+1}W[k])$ for the intermediate reduction map. Using the Greenberg transform, $\rho_{m,n}$ may be regarded as a map of schemes over k . If $Z \subseteq X(W[k])$ is a closed subset of $X(W[k])$, then we say that Z is *finite dimensional* if for every natural number n the set $\rho_n(Z)$ is the set of k -rational points on a subvariety of $\rho_n(X(W[k]))$ with respect to the identification $X(W[k]/p^{n+1}W[k])$ with the k -rational points of an algebraic variety over k and $\limsup \deg \rho_{n+1,n} \upharpoonright (\rho_{n+1}Z)$ is finite.

At least when the characteristic of k is not two, Buium establishes that in analogy to the group homomorphisms constructed by Manin using derivations on function fields that if A is an abelian scheme over $W[k]$ of relative dimension g , then there is a group homomorphism given by a p -differential function $\mu: A(W[k]) \rightarrow W[k]^g$ for which the kernel, $A^\sharp(W[k])$, is finite dimensional. While the actual A^\sharp groups need not vary uniformly, Buium does observe with Remark (1) on page 327 of [6] that the data required to produce group homomorphisms with finite dimensional kernels is bounded uniformly. Let us reformulate his observation as a theorem.

Theorem 4.5 (Buium). *Let k be an algebraically closed field of characteristic $p > 2$. Suppose that S is a variety (reduced, integral scheme of finite type) over $W[k]$ and that $A \rightarrow S$ is an abelian scheme over S of relative dimension g . Then there is a p -differential function $\mu: A(W[k]) \rightarrow W[k]^g$ such that for each $s \in S(W[k])$ the*

map $\mu_s : A_s(W[k]) \rightarrow W[k]^g$ is a group homomorphism for which $\ker(\mu_s)$ is a finite dimensional proalgebraic group.

Since the additive group is torsion free, the group $\ker(\mu_s)$ contains the torsion group $A_s(W[k])_{\text{tor}}$. Moreover, since μ is a p -differential function, the group $\ker(\mu_s)$ is definable in $\mathcal{L}(\mathcal{A}, \sigma)$. In the notation of Theorem 4.1, one might like to argue that there are boundedly many points in $(X_s(W[k]) \setminus \text{Ueno}(X_s)(W[k])) \cap \ker(\mu_s)$ and then conclude *a fortiori* that the same is true with $\ker(\mu_s)$ replaced by the torsion subgroup of $A_s(W[k])$. Unfortunately, this stronger assertion is false in general. However, we shall establish a weak form of this boundedness statement for finite dimensional subgroups of abelian varieties from which Theorem 4.1 follows.

Theorem 4.6. *Let k be an algebraically closed field of characteristic p . Suppose that A is an abelian scheme over $W[k]$. Suppose $G \leq A(W[k])$ is a finite dimensional $\mathcal{L}(\mathcal{A}, \sigma)$ -definable subgroup of $A(W[k])$. If $X \subseteq A$ is a closed subscheme, then $\rho_0((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G)$ is finite.*

Proof. If there were a counter-example to this theorem, then one could be found with $k = \mathbb{F}_p^{\text{alg}}$. Indeed, by the quantifier elimination part of Theorem 3.4 the set $\rho_0((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G)$ is constructible. Hence, if it is infinite it contains a component of the form $Y(k) \setminus F(k)$ where Y is an irreducible variety over k of dimension at least one and F is a proper subvariety. Since the extension $W[\mathbb{F}_p^{\text{alg}}] \hookrightarrow W[k]$ is elementary, the assertion that there exist the appropriate parameters to define such an A , X , G , Y , and F is true in $W[\mathbb{F}_p^{\text{alg}}]$. Likewise, if k' is an algebraically closed field of characteristic p , then because $W[\mathbb{F}_p^{\text{alg}}] \hookrightarrow W[k']$ is elementary, we may transfer the counterexample from $W[\mathbb{F}_p^{\text{alg}}]$ to $W[k']$. Thus, we may take k to be any algebraically closed field of characteristic p .

Let Y be as in the previous paragraph. Let $Z \subseteq Y$ be a curve with $Z(k) \cap F(k)$ finite. Translating, we may assume that Z contains the origin. Let H be the algebraic group generated by Z and let $\tilde{H} := (\rho_0^{-1}H(k)) \cap G$. Then \tilde{H} is a definable, finite dimensional group for which $\rho_0((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap \tilde{H})$ is infinite. Thus, we may and do assume that $G = \tilde{H}$.

We now transpose the proof of Proposition 4.4 of [12] to our unstable situation. For the moment we make use of our flexibility in the choice of k by taking k to be an algebraically closed field of characteristic p and cardinality strictly greater than that of the continuum. For each definable set $T \subseteq \ker(\rho_0 \upharpoonright G)$, let $R_T := \{x \in Z(k) \mid (\exists g \in G) g + T = ((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G)_x\}$. The set R_T is a definable subset of the k -rational points of the curve Z and is thus either finite or cofinite. As $Z(k) = \bigcup_T R_T$ and there are at most continuum many such T and $|Z(k)| > 2^{\aleph_0}$, there must be some T for which R_T is cofinite. Translating T within $\ker(\rho_0 \upharpoonright G)$, we may assume that T contains the origin. Let $S := \{x \in \ker(\rho_0 \upharpoonright G) \mid x + T = T\}$. If $g + T$ is a fibre of $((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G)$, then $g + \bar{S} \subseteq X$ showing that g belongs to the Ueno locus of X unless S is finite, but g does not belong to the

Ueno locus of X . Thus, S must be finite. Thus, the correspondence which associates to $x \in Z(k)$ the g for which $g + T = ((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G)_x$ is one to finite. Let \tilde{Z} be the image of this correspondence in G . Note that \tilde{Z} is a subset of $((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G)$.

As the restriction of the map ρ_0 to \tilde{Z} is finite to one, for $n \gg 0$ the map $\rho_{n+1,n}: \rho_{n+1}(\tilde{Z}) \rightarrow \rho_n(\tilde{Z})$ is a bijective morphism. Thus, we can find finitely many definable subsets $\tilde{Z}_1, \dots, \tilde{Z}_m$ of \tilde{Z} for which $\rho_n(\tilde{Z}_i)$ is always irreducible. For each such “component” if we translate \tilde{Z}_i so that it contains the origin and then form the group L_i that it generates, we see that L_i is definable. Indeed, by the finite dimensionality of G the constructible sets $\rho_n(\tilde{Z}_i)$ generate an algebraic subgroup of $\rho_n(G)$ in a bounded number of steps. As the map ρ_0 is finite to one on \tilde{Z}_i , the same is true on L_i .

Now we use our flexibility in the choice of k to make k small: if $k = \mathbb{F}_p^{\text{alg}}$, then every element of $\rho_0(L_i)$ is torsion. As the kernel of ρ_0 on L_i is finite, it follows that every element of L_i is torsion. By Raynaud’s theorem, $L_i \cap ((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G)$ is finite. As this is true for each i , we conclude that the curve Z in question does not actually exist and that $\rho_0(((X(W[k]) \setminus \text{Ueno}(X)(W[k])) \cap G))$ is finite after all. \square

We are now in a position to complete the proof of Theorem 4.1.

Proof. Let $\mu: A(W[k]) \rightarrow W[k]^g$ be the p -differential function given by Theorem 4.5. By Theorem 4.6 each of the sets $\rho_0((X_s(W[k]) \setminus \text{Ueno}(X_s)(W[k])) \cap \ker(\mu_s))$ is finite. By the quantifier elimination part of Theorem 3.4, this family of finite sets which *prima facie* is uniformly definable only in $W[k]$ is, in fact, uniformly definable in k . The quantifier “there exists infinitely many” may be eliminated in algebraically closed fields. Thus, there is a number B for which each of the above finite sets has cardinality at most B . Thus, the torsion points on X_s but outside the Ueno locus are contained in at most B cosets of the kernel of reduction. There is a bound $M = M(g, p)$ on the number of unramified torsion points in the kernel of reduction on an abelian scheme of relative dimension g depending just on g and p . Thus, there are at most $N := M \cdot B$ torsion points of $A_s(W[k])$ on X_s but outside the Ueno locus. \square

References

- [1] Ax, J., Kochen, S., Diophantine problems over local fields. I. *Amer. J. Math.* **87** (1965), 605–630.
- [2] Ax, J., Kochen, S., Diophantine problems over local fields. II. A complete set of axioms for p -adic number theory. *Amer. J. Math.* **87** (1965), 631–648.
- [3] Ax, J., Kochen, S., Diophantine problems over local fields. III. Decidable fields. *Ann. of Math.* (2) **83** (1966), 437–456.
- [4] Basarab, Ş., Kuhlmann, F.-V., An isomorphism theorem for Henselian algebraic extensions of valued fields. *Manuscripta Math.* **77** (2–3) (1992), 113–126.

- [5] Bélair, L., Macintyre, A., Scanlon, T., Model theory of Frobenius on Witt vectors. Preprint, 2002.
- [6] Buium, A., Differential characters of abelian varieties over p -adic fields. *Invent. Math.* **122** (2) (1995), 309–340.
- [7] Chatzidakis, Z., Hrushovski, E., Model theory of difference fields. *Trans. Amer. Math. Soc.* **351** (8) (1999), 2997–3071.
- [8] Chatzidakis, Z., Hrushovski, E., Peterzil, Y., Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics. *Proc. London Math. Soc.* (3) **85** (2) (2002), 257–311.
- [9] Denef, J., van den Dries, L., p -adic and real subanalytic sets. *Ann. of Math.* (2) **128** (1) (1988), 79–138.
- [10] Hazewinkel, M., *Formal groups and applications*. Pure Appl. Math. 78, Academic Press, Inc., New York, London 1978.
- [11] Hodges, W., *Model Theory*. Encyclopedia Math. Appl. 42, Cambridge University Press, Cambridge 1993.
- [12] Hrushovski, E., The Mordell-Lang conjecture for function fields. *J. Amer. Math. Soc.* **9** (3) (1996), 667–690.
- [13] Hrushovski, E., Proof of Manin’s theorem by reduction to positive characteristic. In *Model theory and algebraic geometry*, Lecture Notes in Math. 1696, Springer-Verlag, Berlin 1998, 197–205.
- [14] Kuhlmann, F.-V., Quantifier elimination for Henselian fields relative to additive and multiplicative congruences. *Israel J. Math.* **85** (1–3) (1994), 277–306.
- [15] Lipshitz, L., Robinson, Z., Uniform properties of rigid subanalytic sets. *Trans. Amer. Math. Soc.* **357** (11) (2005), 4349–4377.
- [16] Raynaud, M., Sous-variétés d’une variété abélienne et points de torsion. In *Arithmetic and geometry*, Vol. I, Progr. Math. 35, Birkhäuser Boston, Boston, MA, 1983, 327–352.
- [17] Scanlon, T., Quantifier elimination for the relative Frobenius. In *Valuation theory and its applications* (Saskatoon, SK, 1999), Vol. II, Fields Inst. Commun. 33, Amer. Math. Soc., Providence, RI, 2003, 323–352.
- [18] Scanlon, T., Local André-Oort conjecture for the universal abelian variety. *Invent. Math.* **163** (1) (2006), 191–211.
- [19] van den Dries, L., Analytic Ax-Kochen-Ersov theorems. In *Proceedings of the International Conference on Algebra* (Novosibirsk, 1989), Part 3, Contemp. Math. 131, Amer. Math. Soc., Providence, RI, 1992, 379–398.
- [20] van den Dries, L., Haskell, D., Macpherson, D., One-dimensional p -adic subanalytic sets. *J. London Math. Soc.* (2) **59** (1) (1999), 1–20.

University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley,
CA 94720-3840, U.S.A.

E-mail: scanlon@math.berkeley.edu